Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Public Safety and Homeland Security Bureau	)	PS Docket No. 19-254
Seeks Comment on Petitions Filed by the	)	
Boulder Regional Emergency Telephone Service	)	
Authority	)	

To: Lisa M. Fowlkes, Chief
Public Safety and Homeland Security Bureau

REPLY COMMENTS OF SAN LUIS AVIATION, INC. dba ESCHAT

San Luis Aviation, Inc. dba ESChat ("ESChat"), through counsel and pursuant to Section 1.405(b) of the Commission's Rules, 47 C.F.R. §1.405(b), hereby respectfully submits its Reply Comments in the above-referenced proceeding. ESChat, as a provider of an "over-the-top" communication service for public safety users, takes this opportunity to correct certain misunderstandings by the Petitioner and some Commenters.

I. BACKGROUND

ESChat is the leading provider of carrier independent Secure Broadband Push-to-Talk ("PTT") services. ESChat service includes AES-256 encrypted PTT voice and multimedia messaging. ESChat also provides live and historical (bread crumb) tracking and mapping. ESChat is approved for U.S. military operational use by the Defense Information Systems Agency ("DISA"). ESChat is a FirstNet Certified™ solution, enhanced by Quality of Service, Priority and Preemption ("QPP") available to FirstNet subscribers. ESChat also supports Quality of Service ("QoS") and RAN priority enhancements on the Verizon Wireless and AT&T commercial networks.

Currently used by all branches of the U.S. Military, as well as federal, state and local public safety agencies, ESChat is able to operate over and across any wireless network, including all commercial carriers, private 3G/4G/5G networks and WiFi. ESChat supports standards-based interoperability with LMR radio networks, including P25 via the native Inter RF Subsystem Interface ("ISSI") protocol and DMR via the native Application Interface Specification ("AIS") protocol. ESChat also supports interoperability via RoIP to all LMR radio networks, regardless of radio technology or operating frequency band.

ESChat is an Over The Top ("OTT") PTT solution that is committed to providing full interoperability, including:

- **Inter-Carrier Interoperability:** Native PTT communication between public safety users operating on different wireless carriers and/or WiFi Networks, and without the need for costly third party [hardware or software] gateway products.
- **Inter System Interoperability:** Secure PTT communication between ESChat users on broadband networks (3G, 4G, 5G, WiFi) and narrow-band LMR networks, regardless of LMR technology or operating frequency band, utilizing standards-based interfaces to ensure reliable and interoperable communications.
- **Inter-Vendor Interoperability:** PTT communication between ESChat and any other broadband PTT product, including 3GPP MCPTT through the use of standards-based interfaces to ensure reliable and interoperable communications.

ESChat has been awarded a contract to provide broadband push-to-talk services for the City of Boulder, Colorado, including ISSI integration and voice encryption to the City's P25 LMR Network. For these reasons, ESChat has a significant interest in this proceeding.

II. REPLY COMMENTS

This proceeding primarily revolves around the use of OTT applications. In contrast to Carrier Integrated PTT solutions, OTT solutions natively facilitate cross carrier PTT service without the need for third party interoperability service or gateways. As a result, OTT PTT service allows public safety agencies to choose the wireless carrier(s) that best meet the needs of the particular agency. It should also be noted that "Carrier Integrated" does not mean interoperability.

Three of the four major US carriers offer commercial Carrier Integrated PTT service from the same vendor, yet none of the carriers support inter-carrier PTT interoperability.

Initially, ESChat wishes to state its belief that the public safety marketplace should have a variety of interoperability solutions, OTT and otherwise, from a variety of solution providers. Ensuring a viable and competitive marketplace will ensure that the best, most secure, and most full-featured options will be available at the lowest possible cost.

With that mission in mind, it is perhaps instructive to first review a few key points regarding the Third Generation Partnership Project ("3GPP") specification for Mission Critical Push-to-Talk ("MCPTT").

- 3GPP's use of the term 'Mission Critical' as it relates to its MCPTT specification represents a marketing term rather than a technical specification for an end-to-end solution that is required to declare a system as mission critical.
- Today's LMR systems represent the benchmark for mission critical systems. They provide an end-to-end solution from the infrastructure to the user.
- The 3GPP MCPTT specification defines a 'server', 'client' and 'interface to a carrier core', rather than a mission critical end-to-end solution. It is an application layer specification, not a full system specification.
- 3GPP MCPTT is a Carrier Integrated PTT architecture.
- Currently there are no 3GPP MCPTT compliant commercial systems operating anywhere in the world.
- Unlike LMR, 3GPP MCPTT requires components including smartphones, smartphone operating systems, smartphone accessories, MCPTT client and server software, and an 'enhanced' commercial wireless network. Without the end-to-end control over the system components, it is not possible to declare MCPTT as mission critical in the same sense as the LMR baseline.

It should be noted that OTT PTT solutions are not only promising interoperability across carriers, solutions like ESChat have been delivering carrier interoperable PTT communications to public safety since 2008, servicing their mission critical needs, contrary to the belief of some commenters.[1] With no 3GPP MCPTT compliant commercial systems operating anywhere in the

[1] In addition, it is not clear to ESChat what "damage" to MCPTT could be caused through proprietary OTT PTT solutions. *See*, for example, the Comments of *Ryan Poltermann*.

world today, OTT PTT applications such as ESChat represent the only proven, secure solution to serve this vital need.

ESChat appreciates the desire of many parties to have direct, core-to-core inter-carrier MCPTT service.[2] In the absence of that service being provided today (or ever), OTT PTT solutions guarantee inter-carrier interoperability, which is among the highest priorities for first responders. The availability of OTT PTT solutions offer a competitive and interoperable option to FirstNet's future MCPTT solutions. As the FirstNet Authority rightly points out in their response, 'FirstNet built by AT&T' is under no obligation to provide inter-carrier and inter-system (LMR) interoperability.[3] In the absence of such an alternative, OTT PTT solutions provide the only option for users, including public safety, to access both inter-carrier and inter-system interoperability.[4]

The Comments submitted by Ryan Poltermann state that:

> Exacerbating this issue is that an OTT solution may be MCPTT on an alternative carrier but may have App Priority on AT&T, which provides not only a confusing picture for public safety agencies but demonstrates that MCPTT on FirstNet alone offers little value for the public safety agency.[5]

It is ESChat's position that public safety must be able to choose the wireless service provider or providers that best suits their needs. OTT PTT solutions offer the only option for wireless provider independent communications. OTT PTT solutions that are able to take advantage of wireless carrier enhancements, such as: QoS, RAN priority and preemption as offered by Verizon and FirstNet. This approach provides public safety the most diverse and enhanced method for secure, reliable and interoperable PTT communications. As such, OTT PTT should not be characterized as 'confusing' the environment for public safety.

---

[2] *Id.*
[3] *FirstNet Authority* Comments at 7.
[4] *AT&T Comments at 13*.
[5] *Poltermann at 2.*

Finally, Verizon states that:

> Full interoperability requires reciprocal commitments and capabilities, which Verizon is already building into its services and networks and is prepared to offer through the use of open standards. Open standards already exist via the 3GPP standards for Mission Critical Push-to-Talk ("MCPTT"), which cover voice, text, data and video services.[6]

ESChat respectfully disagrees. While open standards may be desirable for a host of reasons, "full interoperability" does not have such requirements. Specifically, OTT PTT solutions have been providing full inter-carrier, inter-system interoperability and inter-vendor interoperability for over a decade to public safety agencies. The list of users includes the US military, as well as federal, state and local first responders.

III. CONCLUSION

It is ESChat's fervent hope that the information contained in these Reply Comments will help the Commission and carriers develop rules and policies that will maximize interoperability, maximize user choice and maximize security. ESChat stands ready to work with the Commission, industry and public safety to make that happen.

[6] *Verizon Comments at 6.*

WHEREFORE, the premises considered, it is respectfully requested that the Commission act in accordance with the views expressed herein.

Respectfully submitted,

SAN LUIS AVIATION, INC. dba ESChat

By: Alan S. Tilles, Esquire

Its Attorney

SHULMAN ROGERS GANDAL PORDY & ECKER, P.A.
12505 Park Potomac Ave., Sixth Floor
Potomac, Maryland 20854
(301) 230-5200

Date: October 11, 2019